A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.	
Bureau Name	**FY03 IT Security Spending ($ in thousnds)**
Agency Total	

Inspectors General were not expected to respond to this question.

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.

	FY03 Programs		FY03 Systems		FY03 Contractor Operations or Facilities	
Bureau Name	Total Number	Number Reviewed*	Total Number	Number Reviewed*	Total Number	Number Reviewed*
Region 1	1		1	0	0	
Region 2	1		1	0	0	
Region 3	1		1	0	0	
Region 4	1		1	0	4	
Region 5	1		3	1	6	
Region 6	1		2	0	0	
Region 7	1		1	0	0	
Region 8	1		2	2	1	
Region 9	1		1	0	0	
Region 10	1		1	0	4	
OA	1		2	1	0	
OAR	1		20	6	5	
OARM	1		12	1	1	
OCFO	1		16	10	4	
OECA	1		12	12	0	
OEI - Central **	2		32	9	8	
OEI - Non Central						
OGC	1		1	1	0	
OIA	1		1	0	0	
OIG	1		9	1	0	
OPPTS	1		7	2	3	
ORD	1		19	5	36	
OSWER	1		8	3	5	
OW	1		11	2	0	
Agency Total	24	0	164	56	77	0

b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes	**X**	No	

c. If yes, what methods are used? If no, please explain why.	EPA developed the ASSERT system, which is an automated tool to assist managers in gathering system data in support of the annual FISMA report. The self assessment process is based on NIST Special Publication 800-26. Also, EPA routinely monitored and scored program office compliance with local area network security standards. In addition, EPA conducted document reviews of security plans and network penetration tests. At the Agency's request, the OIG is reviewing the security self assessment process to ensure (a) EPA identified all general support and major application systems, (b) the self-assessments were accurate and complete in accordance with NIST guidance; and (c) major application systems used authentication and identification controls to ensure the systems were protected from unauthorized access or misuse. This review is on-going, with an expected report date in the first quarter of FY2004.			
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes	**X**	No	
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	Yes		No	
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.	The Agency developed the ASSERT system which it uses as the security systems inventory. The Agency is developing a single authoritative information resource registry.			

*The numbers reported reflect programs, systems, and contractor facilities that the OIG reviewed.

** The OIG did not differentiate between OEI - Central and OEI - Non-Central and, therefore, reported all systems reviewed under OEI-Central.

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.

	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
Agency Total				

In FY03, EPA had no material weaknesses in policies, procedures, or practices involving security issues.

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	**Yes**	**No**
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	**X**	
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	**X**	
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	**X**	
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	**X**	
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	**X** The OIG will take an active role in developing a plan to validate the Agency's IT security remediation efforts using the POA&Ms. This validation process will be a joint effort between OEI's Technical Information Security Staff and the OIG.	
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.	**X**	
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.	**X** The OIG was given Super User access to EPA's ASSERT system which includes a module for the POA&Ms. Using the POA&Ms, the OIG will develop a plan to validate the Agency's IT security remediation efforts. This validation process will be a joint effort between OEI's Technical Information Security Staff and the OIG.	

The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		**X** The POA&M database includes a field identifying the targeted completion date. However, the database does not 'prioritize' corrective actions, per se. OEI officials stated that the completion date represents a prioritization. We disagree with OEI's interpretation because while the completion date is a target date to fix the weakness, it does not represent the criticality of

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	The Agency Head took the following steps to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the CIO and EPA program officials. (1) In December 2001, EPA issued a revised Delegations Manual identifying CIO responsibilities and authority (EPA Delegation 1-84, Information Resources Management, dated 12/18/2001). (2) The CIO re-delegated certain responsibilities to various OEI Directors under the authority of EPA Directive 1-84. For example, the CIO re-delegated the Senior Agency Information Security Official responsibilities to the Deputy CIO for Technology. (3) EPA Order 2195.1A4, Agency Network Security Policy, gave the CIO and Deputy CIO responsibilities to establish and enforce the Agency's information security program. In conjunction with the POA&Ms, OEI uses a quarterly reporting process to monitor progress in correcting computer security weaknesses. In addition, OEI's Quality Information Council communicates information security management issues to senior EPA officials. Finally, the Agency maintains a weekly report of computer security incidents.
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	The Agency has made enhancements to both the Capital Planning and Investment Control (CPIC) process and its IT Cost Accounting procedures. The implementation and adherence to these processes and procedures provides reasonable assurance that operating components can not make major IT investments without the review and concurrence of the CIO. However, not all IT expenditures are currently captured by the CPIC process. Expenditures on non-major systems are not subject to the Agency-level CPIC process, but still represent a significant (44%) of the Agency's total IT portfolio. However, non-major systems spending is subject to reporting on the Exhibit 53 and is captured through Agency cost accounting codes. These compensating controls help to provide reasonable assurance that investments are not made without review and concurrence by CIO.
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	The CIO ensures the Agency's information security plan is practiced throughout the life cycle of each agency system, as delegated by the Agency head. Specifically, CIO staff reviewed selected security plans for completeness and worked with program offices to devleop POA&Ms when weaknesses were present. For more information on Agency actions, refer to Question B.4.

B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?	During the reporting period, the following specific actions were taken to oversee the performance of the Agency program offices. The CIO staff reviewed the completeness of the security plans of all systems covered under the CPIC process and when weaknesses were found, program offices developed POA&Ms to mitigate risks. In addition, before a system can be deployed to the Agency's central infrastructure, the system must comply with the Agency's security requirements. However, this review is limited to "Major Agency Systems" or applications that contain data defined as having a high sensitivity. EPA does not verify the existence of security plans for those systems and applications that do not fall into these categories. EPA's current System Life Cycle Management Policy (SLCMP) requires system owners to identify security control methodologies during the design phase of the system life cycle, and to test the effectiveness of these controls before the systems go into production. EPA is revising its SLCMP. The draft policy requires system security planning to begin in the initial phase of system life cycle development by designating or revising information sensitivity levels, conducting a risk assessment, and developing a baseline security plan.

B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)?	EPA has taken steps to integrate its critical infrastructure protection responsibilities with its other security programs. EPA's Office of Environmental Information, Office of Solid Waste and Emergency Response, and Office of Administration and Resources Management all have key roles in the management of EPA's information technology security program. Also, EPA recently established the Office of Homeland Security to be responsible for fostering collaboration in achieving the Agency Critical Infrastructure Protection goals. OIG audit report 2003-P-00009, entitled *EPA Undertaking Implementation Activities to Protect Critical Cyber-Based Infrastructures, Further Steps Needed* , confirms that EPA has taken actions to protect its critical cyber-based infrastructure. However, the report recommends EPA take additional steps by specifically (1) ensuring all sites have required data backup procedures, and (2) providing sufficient resources to complete planned corrective actions to mitigate vulnerabilities previously identified by the General Accounting Office. EPA also needs to establish or revise security plans for IT systems critical to its cyber-based infrastructure so that they meet National Institute for Standards and Technology requirements. In addition, critical IT components of Agency Continuity of Operations Plans need to be tested under circumstances relative to actual deployment. However, the OIG just released an evaluation report entitled *EPA Needs to Assess the Quality of Vulnerability Assessments Related to the Security of the Nation's Water Supply* (Report No. 2003-M-00013). The report states that EPA should promptly analyze the vulnerability assessments submitted by large utilities pursuant to the Bioterrorism Act, to determine whether they adequately address terrorist threats. Electronic or computer systems are one of the six elements utilities must address in their vulnerability assessments.
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	EPA has separate staffs devoted to other security programs under the authority of various Agency officials. Based on the descriptions of the assigned responsibilities, they do not appear to overlap or cause duplication of effort. In addition, EPA's newly created Office of Homeland Security is responsible for ensuring that policies and procedures are consistent and complimentary across EPA's various programs and disciplines.

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its national critical operations and assets?	Yes		No	X
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	Yes		No	X
c. Has the agency fully identified its mission critical operations and assets?	Yes	X	No	
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	Yes	X	No	
e. If yes, describe the steps the agency has taken as a result of the review.	With respect to its critical IT infrastructure, EPA has addressed vulnerablilties identified during risk assessments, established suitable emergency management procedures, and established effective internal and external interagency coordination.			
f. If no, please explain why.	In May 2002, EPA completed a draft Project Matrix, Step 1 Report, which preliminarily identified its national critical operations and assets. However, that report has not been finalized because the Department of Homeland Security refined its approach to Project Matrix. In response to this shift in methodology, EPA is currently identifying its critical functions, services, and products. In the Fall of 2003, in coordination with program officials, EPA's Office of Homeland Security plans to commence identification of the interdependencies and interrelationships of nationally critical functions, services, and products.			

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	Incidents with criminal ramifications are reported to the OIG's Computer Crimes Directorate (CCD). The CCD reports such incidents to external law enforcement authorities as they deem appropriate. The Agency provides a weekly incident report to FedCIRC.			
b. Total number of agency components or bureaus.	24			
c. Number of agency components with incident handling and response capability.	24			
d. Number of agency components that report to FedCIRC.	1, because EPA has a centralized reporting process			
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	Yes. The Agency provides a weekly incident report to FedCIRC.			
f. What is the required average time to report to the agency and FedCIRC following an incident?	Weekly			
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	The EPA utilizes a Centralized Computer Security Incident Response Capability (CSIRC) team for vulnerability patch notification and tracking. The CSIRC utilizes the FedCIRC Patch Authentication and Dissemination Capability (PADC) tool along with other vulnerability notification resources. CSIRC reviews the vulnerability notifications and then sends alerts to EPA National Technology managers. The technology managers test the patches and provide instructions for patch installation and location. CSIRC then provides notification to Agency Security Officers who ensure patches are installed and provide responses on patch status. CSIRC tracks patch installation status for the EPA.			
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes	**X**	No	
i. If yes, how many active users does the agency have for this service?	10			
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes	**X**	No	
k. Do these configuration requirements address patching of security vulnerabilities?	Yes	**X**	No	

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.

Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC or law enforcement
OA	2	2
OAR	3	3
OARM	15	15
OCFO	6	6
OECA	5	5
OEI - Non Central	44	44
OEI - Central	2,700,000 *	2,700,000
OGC	0	0
OIA	0	0
OIG	6	6
OPPTS	4	4
ORD	22	22
OSWER	0	0
OW	2	2
Region 1	7	7
Region 2	4	4
Region 3	3	3
Region 4	6	6
Region 5	9	9
Region 6	10	10
Region 7	2	2
Region 8	13	13
Region 9	2	2
Region 10	6	6

* This number includes *un* successful hits against the Agency's perimeter defenses.

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Region 1	1														
Region 2	1														
Region 3	1														
Region 4	1														
Region 5	3														
Region 6	2														
Region 7	1														
Region 8	2														
Region 9	1														
Region 10	1														
OA	2														
OAR	20														
OARM	12														
OCFO	16														
OECA	12														
OEI - Central	12														
OEI - Non Central	20														
OGC	1														
OIA	1														
OIG	9														
OPPTS	7														
ORD	19														
OSWER	8														
OW	11														
Agency Total	164														

The OIG is in the process of conducting an audit of EPA's security self-assessment process. Specifically, this audit's objectives include determining whether (a) EPA had identified all general support and major application systems, (b) the self-assessments were accurate and complete; and (c) major application systems used authentication and identification controls to ensure the systems were protected from unauthorized access or misuse. Preliminary results indicated that (a) some program offices within EPA had not identified all major application systems, (b) 27% of the sampled self assessment questions were unsupported and approximately 9% of the sampled questions were inaccurate; and (c) EPA did not adequately plan for identification and authentication controls.

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.				
Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
Yes	**Yes**		**Yes**	**Yes**
The CIO maintains an Agency-wide security program that is managed by security staff within OEI's Office of Technology Operations and Planning (OTOP). OTOP manages EPA's IT infrastructure which supports information services, such as the management of Headquarters local area networks and the EPA website. OTOP's security staff also develop and implement IT policies and plans for information security, and oversee the implementation of the security program.	All agency program offices performed self assessments through EPA's ASSERT system. OEI's security staff created POA&Ms for significant security weaknesses and tracked program office corrective actions. OEI also evaluates agency performance by conducting network penetration tests. In addition, OEI uses automated tools to assess local area network compliance with security standards and provides quarterly reports to regional and program offices.	Each program office is required to input data into the ASSERT system, which is based on NIST Special Publication 800-26. The CIO uses this data to support the annual FISMA report. In addition, OEI's security staff use ASSERT to track progress on correcting significant system deficiencies.	The Technical Information Security Staff (TISS) is responsible for managing the Agency's IT security program. TISS' key program components include: IT security planning, program management, evaluation of effectiveness, support to other programs, support for policy & procedure development, communications, and acting as the Information Security Officer for OTOP.	The ASSERT system automatically generates POA&Ms based on the answers program offices provide to the security self-assessment questions. In addition, ASSERT allows users to input and track security weaknesses stemming from additional reviews, including those performed by the Inspector General and General Accounting Office.

	C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?							
	Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
		Number	Percentage		Number	Percentage		
OA	699	690	98.7%	7	2	28.6%		$0.00
OAR	1312	1312	100.0%	76	30	39.5%	2002 ISO, Sr.Ex/Mgt., 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Other	$ 68,472.00
OARM	777	777	100.0%	30	14	46.7%	2002 ISO, New Empl. Orien., Sr. Ex/Mgt, 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Tech. Cert. Mgt., Other	$ 38,189.00
OCFO	341	341	100.0%	65	11	16.9%	2002 ISO, 2003 ISO, DB Mgt.	$ 14,442.00
OECA	920	920	100.0%	23	6	26.1%	2002 ISO, 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Tech. Cert. Mgt., Other	$ 52,700.00
OEI	413	394	95.4%	95	22	23.2%	2002 ISO, Sr.Ex/Mgt., 2003 ISO, P/R Sec. Awr., Sec. Mgt., Syst. Mgt., Tech. Cert. Mgt., Other	$ 513,821.00
OGC	206	204	99.0%	4	1	25.0%	2002 ISO, 2003 ISO	$ 1,501.00
OIA	88	88	100.0%	2	1	50.0%	2002 ISO, 2003 ISO, Sec. Mgt., DB Mgt.	$ 4,500.00
OIG	360	313	86.9%	17	3	17.6%	Sec. Mgt., Syst. Mgt., DB Mgt., Tech. Cert. Mgt., Other	$ 22,000.00
OPPTS	1434	1318	91.9%	22	4	18.2%	2002 ISO, Sr.Ex/Mgt., 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Tech. Cert. Mgt.	$ 60,027.00
ORD	2996	2885	96.3%	62	9	14.5%	2002 ISO, New Empl. Orien., 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Tech. Cert. Mgt.	$ 33,925.00
OSWER	634	634	100.0%	36	28	77.8%	2002 ISO, Sr.Ex/Mgt., 2003 ISO, Syst. Mgt., DB Mgt., Tech. Cert. Mgt., Other	$ 24,600.00
OW	750	664	88.5%	18	5	27.8%	2003 ISO	$ 1,000.00
Region 1	740	740	100.0%	30	4	13.3%	2002 ISO, 2003 ISO, Sec. Mgt., Syst. Mgt.,	$ 10,928.00
Region 2	1135	1120	98.7%	18	3	16.7%	2002 ISO, 2003 ISO, Syst. Mgt, DB Mgt.	$ 19,600.00
Region 3	992	845	85.2%	22	2	9.1%	2002 ISO, 2003 ISO, DB Mgt., Tech Cert. Mgt.	$ 9,800.00
Region 4	1389	1251	90.1%	15	10	66.7%	Syst. Mgt., Tech. Cert. Mgt.	$ 4,500.00
Region 5	1479	1454	98.3%	6	3	50.0%	2002 ISO, 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Tech. Cert. Mgt.	$ 48,400.00
Region 6	972	972	100.0%	22	1	4.5%	2002 ISO, 2003 ISO, Tech. Cert. Mgt., Other	$ 26,400.00
Region 7	674	627	93.0%	18	0	0.0%	2002 ISO, 2003 ISO	$ 3,200.00
Region 8	676	676	100.0%	32	30	93.8%	2003 ISO, Syst. Mgt., DB Mgt., Tech. Cert. Mgt., Other	$ 28,258.00

Region 9	976	868	88.9%	25	4	16.0%	Sytex, 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Other	$ 21,100.00
Region 10	650	650	100.0%	9	9	100.0%	2002 ISO, 2003 ISO, Sec. Mgt., Syst. Mgt., DB Mgt., Tech. Cert. Mgt., Other	$ 15,000.00
TOTAL	20,613	19,743	95.78%	654	202	30.89%		$1,022,363.00

We were unable to perform a detailed review of the FY 03 IT security training data because the Agency did not compile this information until mid-September. These time contraints prevented us from validating the accuracy of the information EPA submitted to OMB. However, the OIG plans to validate the FY03 IT security training data during the next FISMA audit cycle.

As part of this year's evaluation, we attempted to validate EPA's FY02 IT security training data for employees with significant security responsibilities. We requested supporting documentation from EPA program offices for these individuals; however, most program offices were unable to provide this information. OEI is in the process of establishing a training system that will aid in the tracking of security training for such employees.

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?				
Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
	26	Yes	Yes	Yes
		EPA's guidance for preparing business cases requested program officials to include security information. EPA received approximately 48 business cases, and we judgmentally sampled 30 of them. Our review indicated that EPA program officials integrated security into these business cases. Time constraints prevented us from reviewing all 48 business cases.	Twenty-six business cases were included in the initial budget submission sent to OMB. These 26 business cases represent IT investments greater than $3 million. Our review corroborated that EPA's CIO integrated security into these business cases.	EPA reported IT security costs for all IT investments in its Exhibit 53, with the exception of two systems that are being phased out (Integrated Resource Management System and Contract Lab Program Support System).

We were unable to obtain and review EPA's business cases and Exhibit 53 until it had aggregated and forwarded the budget submission to OMB. These time constraints prevented us from verifying the accuracy of information reported to OMB. We plan on evaluating and validating this information during the next FISMA audit cycle.

Quarterly POA&M Updated Information	Programs	Systems
a. Total number of weaknesses identified at the start of the quarter.		
b. Number of weaknesses for which corrective action was completed on time (including testing) by the end of the quarter.		
c. Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled.		
d. Number of weaknesses for which corrective action has been delayed including a brief explanation for the delay.		
e. Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.).		

Quarterly IT Security Performance Measures Update															
Bureau Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level or risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested**	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total															